DETAILED ACTION

1. Preliminary Amendment, received on 10 March 2005, has been entered into record. In this amendment, claims 1, 3-7 and 10-13 have been amended, claim 14 has been cancelled, and claims 15-25 have been added.

2. Claims 1-13 and 15-25 are presented for examination.

Priority

3. The claim for priority from PCT/EP02/10400 filed on 13 September 2002 is duly noted.

Information Disclosure Statement

4. The information disclosure statement filed 10 March 2005 fails to comply with 37 CFR 1.98(a)(2), which requires a legible copy of each cited foreign patent document; each non-patent literature publication or that portion which caused it to be listed; and all other information or that portion which caused it to be listed. It has been placed in the application file, but the information referred to therein has not been considered.

Specification

5. The abstract of the disclosure does not commence on a separate sheet in accordance with 37 CFR 1.52(b)(4). A new abstract of the disclosure is required and must be presented on a separate sheet, apart from any other text.

6. The disclosure is objected to because it contains an embedded hyperlink and/or other form of browser-executable code. Applicant is required to delete the embedded hyperlink and/or other form of browser-executable code. See MPEP § 608.01.

7. The disclosure is objected to because of the following informalities: It is unclear if the applicant intended for the “interfaceID’ to read as "interfaceID” (e.g. page 4, line 32) or as “interface ID” (e.g. page 5, line 15).

Appropriate correction is required.

Claim Objections

8. Claims 1-6, 8-13, 15-19, 21-25 are objected to because of the following informalities:

a. In claim 1, line 8: “the IP address” lacks antecedent basis;

b. In claims 2-6, line 1: “A method” is unclear if it relates to “A method” (claim 1, line 1);

c. In claim 3, line 2: “an interfaceID” is unclear if it relates to “an interfaceID” (claim 1, lines 8-9);

d. In claim 3, line 2: "ownIPv6" should read –own IPv6–;

e. In claim 3, line 8: “the member’s private key” lacks antecedent basis;

f. In claim 4, line 8: “the source IP address” lacks antecedent basis;

g. In claims 8-12, line 1: “A method” is unclear if it relates to “A method” (claim 7, line 1);

h. In claim 9, line 2: “a control node” is unclear if it relates to “a control node” (claim 7, line 7);

i. In claim 11, line 5: “the visited network” lacks antecedent basis;

j. In claim 11, line 7: “a certificate” is unclear if it relates to “a certificate” (claim 7, line 4);

k. In claim 11, line 8: “a public-private key pair” is unclear if it relates to “a public private key pair” (claim 7, lines 4-5);

l. In claim 13, line 6: "a group controller" is unclear if it relates to "A group controller" (claim 13, line 1);

m. In claim 13, line 10: “the IP address” lacks antecedent basis;

n. In claims 15-19, line 1: “A group controller” is unclear if it relates to “A group controller” (claim 13, line 1);

o. In claim 17, line 6: “the same cryptographic hash” lacks antecedent basis;

p. In claim 17, line 8: “the source IP address” lacks antecedent basis;

q. In claims 21-25, line 1: “A group controller” is unclear if it relates to “A group controller” (claim 20, line 1);

r. In claim 22, line 2: “a control node” is unclear if it relates to “a control node” (claim 20, line 7);

s. In claim 23, line 6: “the message” lacks antecedent basis;

t. In claim 23, line 7: “the user’s private key” lacks antecedent basis;

u. In claim 24, line 5: “the visited network” lacks antecedent basis;

v. In claim 24, line 7: "a certificate" is unclear if it relates to "a certificate" (claim 20, line 4);

w. In claim 24, line 9: "a public-private key pair" is unclear if it relates to "a public private key pair" (claim 20, lines 4-5).

Appropriate correction is required.

Drawings

9. Figures 1 and 2 should be designated by a legend such as --Prior Art-- because only that which is old is illustrated. See MPEP § 608.02(g).

Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as "amended." If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for consistency. Additional replacement sheets may be necessary to show the renumbering of the remaining figures. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the

applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Claim Rejections - 35 USC § 102

10. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

11. Claims 1, 3-4, 13, 16-17 are rejected under 35 U.S.C. 102(a) as being anticipated by Nikander (GB 2367986 A).

As to claims 1 and 13, Nikander discloses a method for IP network authorization using a coded interface identifier, the method having:

> **at the group controller, verifying that the public key received from each candidate member wishing to participate is owned by that candidate member and that the public key is associated with the IP address of that candidate member by inspecting an interfaceID part of the IP address** (page 8, lines 21-29)**.**

As to claims 3 and 16, Nikander discloses:

> **wherein each candidate member generates an interfaceID part of its ownIPv6 address by taking a cryptographic hash over the candidate member's own public key and one or more other parameters** (page 6, lines

23-27), **and the candidate member sends a joining request to the group controller which contains: the member's IP address including the generated interface ID; the candidate member's own public key; and a signature over the entire message generated using the member's private key** (page 9, lines 3-8).

As to claims 4 and 17, Nikander discloses:

a) uses the received public key to confirm that the signature is valid, thus proving that the candidate member does indeed own the public-private key pair to which the received public key belongs (page 9, lines 3-6)

b) applies the same cryptographic hash, as used by the candidate member, to the public key and the other parameter (s) and compares the result to the interfaceID part of the member's IP address, thus verifying that the source IP address is owned by the candidate (page 9, lines 6-8).

Claim Rejections - 35 USC § 103

12. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

13. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of

the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

14. Claims 2, 5-6, 15, 18-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nikander as applied to claims 1 and 13 above, and in view of Caronni et al. (US Patent 6,049,878 and Caronni hereinafter).

As to claims 2 and 15, Nikander does not disclose:

wherein said key revocation based scheme is a Logical Key Hierarchy based scheme.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Nikander, as evidenced by Caronni.

Caronni discloses a system and method for efficient, secure multicasting with global knowledge, the system and method having:

wherein said key revocation based scheme is a Logical Key Hierarchy based scheme (i.e. binary tree) (col. 6, lines 27-31)**.**

Given the teaching of Caronni, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Nikander with the teachings of Caronni by using a Logical Key

Hierarchy based scheme. Caronni recites motivation by disclosing that using a secure distribution tree can allow scalability (col. 3, lines 12-20). It is obvious that the teachings of Caronni would have improved the teachings of Nikander by using a tree distribution scheme in order to allow for scalability in the system.

As to claims 5 and 18, Nikander does not disclose:

> **wherein, after the group controller has received the public key from a given candidate member and has verified that the public key is associated with the IP address of the sender, the group controller sends a unique Key Encryption Key to the member, encrypted with that member's public key, and the group controller also sends a Traffic Encryption Key and a LKH key set to the member, encrypted with the Key Encryption Key.**

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Nikander, as evidenced by Caronni.

Caronni discloses:

> **wherein, after the group controller has received the public key from a given candidate member and has verified that the public key is associated with the IP address of the sender, the group controller sends a unique Key Encryption Key to the member, encrypted with that member's public key, and the group controller also sends a Traffic Encryption Key and a LKH key set to the member, encrypted with the Key Encryption Key** (col. 6, lines 27-37).

Given the teaching of Caronni, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Nikander with the teachings of Caronni by using multiple keys for encryption. Caronni recites motivation by disclosing that using multiple keys allows for the forming of groups by sharing the KEK with particular participants (col. 8, lines 61-63) while the TEK is shared among all participants (col. 6, lines 16-17). It is obvious that the teachings of Caronni would have improved the teachings of Nikander by using multiple keys for encryption in order to allow the forming of groups within the multicast.

As to claims 6 and 19, Nikander does not disclose:

a one-way multicast where a single node multicasts a stream of data to several other nodes;

a group multicast where group members multicast data to all other members of the group; or

a tele-conference or a videoconference or a multimedia conference.

Nonetheless, these features are well known in the art and would have been an obvious modification of the teachings disclosed by Nikander, as evidenced by Caronni.

Caronni discloses:

a one-way multicast where a single node multicasts a stream of data to several other nodes;

a group multicast where group members multicast data to all other members of the group; or

a tele-conference or a videoconference or a multimedia conference (col. 3, lines 34-43).

Given the teaching of Caronni, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Nikander with the teachings of Caronni by using a one-way multicast, a group multicast or a teleconference. Caronni recites motivation by disclosing that multicasting is an effective platform for building group-oriented services (col. 1, lines 34-36). It is obvious that the teachings of Caronni would have improved the teachings of Nikander by allowing for a one-way multicast, a group multicast, or a teleconferecnce in order to create a platform for effective group-oriented services where participants can communicate with other participants.

15. Claims 7-9, 20-22 and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wesley et al. (US Patent 6,275,859 B1 and Wesley hereinafter) and in view of Caronni.

As to claims 7 and 20, Wesley discloses a system and method for tree-based reliable multicasting, the system and method having:

delivering a certificate to the user, the certificate verifying that a public private key pair identified in the certificate can be validly used by the user to access said secure multicast/broadcast (col. 4, lines 15-22)**;**

subsequently verifying at a control node that the certificate is owned by the user using a proof-of-possession procedure (col. 3, lines 6-9)**.**

Wesley does not disclose:

assuming that verification is obtained, using said public key to send a Key Encryption Key to the user.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Wesley, as evidenced by Caronni.

Caronni discloses:

assuming that verification is obtained, using said public key to send a Key Encryption Key to the user (col. 6, lines 27-31)**.**

Given the teaching of Caronni, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Wesley with the teachings of Caronni by sending a Key Encryption Key to a user. Please refer to the motivation recited above in respect to claims 5 and 18 as to why it is obvious to apply the teachings of Caronni to the teachings of Wesley.

As to claims 8 and 21, Wesley does not disclose:

wherein said key revocation based scheme is a Logical Key Hierarchy based scheme.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Wesley, as evidenced by Caronni.

Caronni discloses:

wherein said key revocation based scheme is a Logical Key Hierarchy based scheme (i.e. binary tree) (col. 6, lines 27-31)**.**

Given the teaching of Caronni, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Wesley with the teachings of Caronni by using a Logical Key Hierarchy based scheme. Please refer to the motivation recited above in respect to claims 2 and 15 as to why it is obvious to apply the teachings of Caronni to the teachings of Wesley.

As to claims 9 and 22, Wesley discloses:

> **wherein said step of verifying at a control node that the certificate is owned by the user, is carried out after the control node receives a request from the user to join said secure multicast or broadcast** (col. 4, lines 3-6).

As to claim 25, Wesley discloses:

> **wherein an Authentication and Key Agreement (AKA) procedure is used to authorise the user** (col. 2, lines 5-13). The examiner asserts that using a symmetric key authentication on a security protocol would have been functionally equivalent to using an Authentication and Key Agreement procedure. Thus, it would have been obvious to modify the teachings of Wesley with an Authentication and Key Agreement procedure in order to obtain the claimed invention.

16. Claims 10 and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wesley in view of Caronni as applied to claims 7 and 20 above, and further in view of Nikander.

As to claims 10 and 23, Wesley in view of Caronni does not disclose:

> **wherein said proof-of-possession procedure involves the control node sending a random number to the user in plain text, and the user sending a response to the control node containing a signature generated by applying the private key to the random number, wherein the control node is in possession of the user's certificate and can check whether or not the message is correctly signed with the user's private key.**

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Wesley in view of Caronni, as evidenced by Nikander.

Nikander discloses:

> **wherein said proof-of-possession procedure involves the control node sending a random number to the user in plain text** (page 8, lines 5-6, 10)**, and the user sending a response to the control node containing a signature generated by applying the private key to the random number** (page 8, lines 16-18)**, wherein the control node is in possession of the user's certificate and can check whether or not the message is correctly signed with the user's private key** (page 9, lines 3-8)**.**

Given the teaching of Nikander, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Wesley in view of Caronni with the teachings of Nikander by using a random number and signature to verify if a message is correctly signed. Caronni recites motivation by disclosing that existing multicasting techniques must be supplemented by tools for protecting (i.e. encrypting and authenticating) traffic, controlling participation, and restricting access from unauthorized users (col. 1, lines 37-40). It is obvious that the teachings of Wesley in view of Caronni would have benefited from the teachings of Nikander by using a random number and signature to verify a message in order to provide protection and security in a multicasting system.

17. Claims 11-12 and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wesley in view of Caronni as applied to claims 7 and 20 above, and further in view of Pellacuru (US Patent 7,334,125 B1).

As to claims 11 and 24, Wesley, combined with Caronni, discloses:

> **following authorisation by the home network, generating a certificate relating to said service and generating a public-private key pair, either at the user equipment or within one of the networks, and signing the certificate** (col. 4, lines 15-22)**;**
>
> **sending the certificate to the user** (col. 4, lines 19-22)**.**

Wesley in view of Caronni does not disclose:

the visited network contacting the user's home network, upon receipt of an initial registration request from said user, to authorise the user.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Wesley in view of Caronni, as evidenced by Pellacuru.

Pellacuru discloses a system and method for facilitating secure communications among multicast nodes in a telecommunications network, the system and method having:

the visited network contacting the user's home network, upon receipt of an initial registration request from said user, to authorise the user (col. 6, lines 4-10)**.**

Given the teaching of Pellacuru, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Wesley in view of Caronni with the teachings of Pellacuru by authorizing a user on a different network. Pellacuru recites motivation by disclosing that multicasting may occur where a user on a local area network is connected to the Internet (col. 3, lines 15-26), allowing a receiver to be located on a different network from the source. It is obvious that the teachings of Pellacuru would have improved the teachings of Wesley in view of Caronni by authenticating a user on a different network in order to allow a user to participate in a multicast where the source is located on a different network.

As to claim 12, Wesley, combined with Caronni and Pellacuru, discloses:

wherein an Authentication and Key Agreement (AKA) procedure is used to authorise the user (col. 2, lines 5-13). The examiner asserts that using a symmetric key authentication on a security protocol would have been functionally equivalent to using an Authentication and Key Agreement procedure. Thus, it would have been obvious to modify the teachings of Wesley with an Authentication and Key Agreement procedure in order to obtain the claimed invention.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Sarah Su whose telephone number is (571) 270-3835. The examiner can normally be reached on Monday through Friday 7:30AM-5:00PM EST..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Sarah Su/
Examiner, Art Unit 2131

/Christopher A. Revak/
Primary Examiner, Art Unit 2131